CLAIMS

We claim:

1. An apparatus for accessing material, comprising:

a secure registry encrypted with a registry key and storing another key useful for decrypting material; and

a control module configured to decrypt said secure registry using said registry key for retrieval of said another key if a correct entity identification is received.

2. The apparatus according to claim 1, wherein said control module receives said material as streaming media, and is further configured to decrypt said material using said another key.

3. The apparatus according to claim 2, wherein said streaming media is in MPEG-4 format encrypted with at least one content key, and said control module receives said at least one content key encrypted with said another key.

4. The apparatus according to claim 3, wherein said another key comprises at least one license key corresponding to a license to use said material.

5. The apparatus according to claim 2, wherein said streaming media is in MPEG-4 format encrypted with at least one content key, and said control module receives said

at least one content key encrypted with a public key of said apparatus.

6. The apparatus according to claim 5, wherein said another key comprises a private key of said apparatus.

7. The apparatus according to claim 1, further comprising a file including an encrypted version of said material, and said another key is useful for decrypting said encrypted version of said material.

8. The apparatus according to claim 7, wherein said material is in MPEG-4 format encrypted with at least one content key, and said at least one content key is provided encrypted with said another key.

9. The apparatus according to claim 8, wherein said another key comprises at least one license key corresponding to a license to use said material.

10. The apparatus according to claim 7, wherein said material is in MPEG-4 format encrypted with at least one content key, and said at least one content key is provided encrypted with a public key of said apparatus.

11. The apparatus according to claim 10, wherein said another key comprises a private key of said apparatus.

12. The apparatus according to claim 1, wherein said control module includes a control program and a replaceable software module linked to said control program so as to provide said registry key to said control program.

13. The apparatus according to claim 12, wherein said replaceable software module is a dynamic link library module.

14. The apparatus according to claim 12, wherein said replaceable software module provides both a new and old registry key to said control program so that said control program can decrypt said secure registry with said old registry key, encrypt said decrypted secure registry with said new registry key, and replace said secure registry encrypted with said old registry key with said secure registry encrypted with said new registry key.

15. The apparatus according to claim 12, wherein said replaceable software module has been provided by and linked to said control program by a server.

16. The apparatus according to claim 1, wherein said registry key is integrated into a binary executable code of said control module.

17. The apparatus according to claim 16, wherein a server has provided said control program to said apparatus.

18. The apparatus according to claim 1, wherein said control module includes a registry key generator that generates said registry key using a sensed entity identification.

19. The apparatus according to claim 18, wherein said sensed entity identification is unique for said apparatus.

20. The apparatus according to claim 18, wherein said sensed entity identification is unique for a hardware device connectable to said apparatus.

21. The apparatus according to claim 18, wherein said sensed entity identification is unique for a user of said apparatus.

22. The apparatus according to claim 1, wherein said control module includes a comparison module that determines whether said correct entity identification has been received by comparing a reference entity identification against a sensed entity identification.

23. The apparatus according to claim 22, wherein said sensed entity identification is unique for said apparatus.

24. The apparatus according to claim 23, wherein said sensed entity identification is a computer identification.

25. The apparatus according to claim 23, wherein said sensed entity identification is a network interface card identification.

26. The apparatus according to claim 23, wherein said sensed entity identification is a hard disk drive identification.

27. The apparatus according to claim 22, wherein said sensed entity identification is unique for a hardware device connectable to said apparatus.

28. The apparatus according to claim 27, wherein said sensed entity identification is a smartcard identification.

29. The apparatus according to claim 27, wherein said sensed entity identification is a content storage unit identification.

30. The apparatus according to claim 22, wherein said sensed entity identification is unique to a user of said apparatus.

31. The apparatus according to claim 30, wherein said sensed entity identification is a credit card number.

32. The apparatus according to claim 30, wherein said sensed entity identification is a predefined user identification.

33. The apparatus according to claim 30, wherein said sensed entity identification is a biometrics based identification.

34. The apparatus according to claim 33, wherein said biometrics based identification is a fingerprint of said user of said apparatus.

35. The apparatus according to claim 33, wherein said biometrics based identification is a speech of said user of said apparatus.

36. The apparatus according to claim 1, wherein a remote server determines whether said correct entity identification is received.

37. The apparatus according to claim 1, wherein said control module comprises a processor and a control program running on said processor.

38. The apparatus according to claim 1, wherein said control module includes logic circuitry.

39. The apparatus according to claim 1, wherein said control module is license-enabled to a unique identification of said apparatus.

40. The apparatus according to claim 1, wherein said secure registry further stores information related to said material.

41. The apparatus according to claim 40, wherein said information related to said material includes usage rights included in a license for said material.

42. A method for accessing material, comprising:

decrypting a secure registry with a registry key;

retrieving another key from said decrypted secure registry; and

decrypting encrypted material using said another key to access said material.

43. The method according to claim 42, further comprising receiving said encrypted material as streaming media.

44. The method according to claim 43, wherein said streaming media is in MPEG-4 format encrypted with at least one content key, and further comprising receiving said at least one content key encrypted with said another key.

45. The method according to claim 44, wherein said decrypting encrypted material using said another key to access said material, comprises:

decrypting said at least one content key with said another key; and

decrypting said encrypted material with said at least one content key to access said material.

46. The method according to claim 45, wherein said another key comprises at least one license key corresponding to a license to use said material.

47. The method according to claim 43, wherein said streaming media is in MPEG-4 format encrypted with at least one content key, and further comprising receiving said at least one content key encrypted with a public key of a recipient of said material.

48. The method according to claim 47, wherein said another key comprises a private key of said recipient of said material.

49. The method according to claim 48, wherein said decrypting encrypted material using said another key to access said material, comprises:

decrypting said at least one content key with said private key; and

decrypting said encrypted material with said at least one content key to access said material.

50. The method according to claim 42, further comprising receiving said encrypted material as a file.

51. The method according to claim 50, wherein said file is in MPEG-4 format encrypted with at least one content key, and further comprising receiving said at least one content key encrypted with said another key.

52. The method according to claim 51, wherein said decrypting encrypted material using said another key to access said material, comprises:

decrypting said at least one content key with said another key; and

decrypting said encrypted material with said at least one content key to access said material.

53. The method according to claim 52, wherein said another key comprises at least one license key corresponding to a license to use said material.

54. The method according to claim 50, wherein said file is in MPEG-4 format encrypted with at least one content key, and further comprising receiving said at least one content key encrypted with a public key of a recipient of said material.

55. The method according to claim 54, wherein said another key comprises a private key of said recipient of said material.

56. The method according to claim 55, wherein said decrypting encrypted material using said another key to access said material, comprises:

decrypting said at least one content key with said private key; and

decrypting said encrypted material with said at least one content key to access said material.

57. The method according to claim 42, further comprising retrieving said registry key from a replaceable software module.

58. The method according to claim 57, further comprising prior to said decrypting encrypted material using said another key to access said material:

receiving a sensed entity identification; and

comparing a reference entity identification against said sensed entity identification;

wherein said decrypting encrypted material using said another key to access said material comprises decrypting encrypted material using said another key to access said material only if said reference entity identification matches said sensed entity identification.

59. The method according to claim 58, wherein said reference entity identification is stored in said secure registry along with said another key.

60. The method according to claim 58, wherein said reference entity identification is provided by said replaceable software module.

61. The method according to claim 42, further comprising retrieving said registry key from binary executable code of a control module.

62. The method according to claim 61, further comprising prior to said decrypting encrypted material using said another key to access said material:

receiving a sensed entity identification; and

comparing a reference entity identification against said sensed entity identification;

wherein said decrypting encrypted material using said another key to access said material comprises decrypting encrypted material using said another key to access said material only if said reference entity identification matches said sensed entity identification.

63. The method according to claim 62, wherein said reference entity identification is stored in said secure registry along with said another key.

64. The method according to claim 62, wherein said reference entity identification is integrated into said binary executable code of said control module along with said registry key.

65. The method according to claim 64, further comprising generating said registry key using a sensed entity identification.

66. The method according to claim 65, wherein said sensed entity identification is unique to a host.

67. The method according to claim 65, wherein said sensed entity identification is unique to a hardware device connectable to a host.

68. The method according to claim 65, wherein said sensed entity identification is unique to a user of a host.

69. The method according to claim 68, further comprising receiving said sensed entity identification from information entered into an input device by said user.

70. The method according to claim 69, wherein said input device is a keyboard.

71. The method according to claim 69, wherein said input device is a biometrics device.

72. The method according to claim 42, further comprising after said decrypting encrypted material using said another key to access said material:

using said material according to a license stored in said secure registry along with said another key.